CLAIMS

1. A method of establishing a session key (K) shared between a first network element (NEa) of a first network domain (100) and a second network element (NEb) of a second network domain (200), said first network domain (100) comprising first cryptographic means (120) and sharing a secret key (K_{AB}) with said second network domain (200) comprising second cryptographic means (220), said method comprising the steps of:

- said first cryptographic means (120) generating a freshness token (FRESH);
- said first cryptographic means (120) generating said session key (K) based on said shared secret key (K_{AB}) and said generated freshness token (FRESH);
- providing said session key (K) to said first network element (NEa);
- providing said freshness token (FRESH) to said second cryptographic means (220);
- said second cryptographic means (220) generating a copy of said session key (K) based on said shared secret key (K_{AB}) and said provided freshness token (FRESH); and
- providing said copy of said session key (K) to said second network element (NEb).

2. A method of enabling secure communication between a first network element (NEa) of a first network domain (100) and a second network element (NEb) of a second network domain (200), said first network domain (100) comprising first cryptographic means (120) and sharing a secret key (K_{AB}) with said second network domain (200) comprising second cryptographic means (220), said method comprising the steps of:

- said first cryptographic means (120) generating a freshness token (FRESH);
- said first cryptographic means (120) generating said session key (K) based on said shared secret key (K_{AB}) and said generated freshness token (FRESH);
- providing said session key (K) to said first network element (NEa);

- providing said freshness token (FRESH) to said second cryptographic means (220);
- said second cryptographic means (220) generating a copy of said session key (K) based on said shared secret key (K_{AB}) and said provided freshness token (FRESH);
- providing said copy of said session key (K) to said second network element (NEb); and
- said first network element (NEa) and said second network element (NEb) securely communicating based on said session key (K) and said copy of said session key (K).

3. The method according to claim 1 or 2, wherein said session key providing step comprises the step of securely providing said session key (K) to said first network element (NEa) and said session key copy providing step comprises the step of securely providing said copy of said session key (K) to said second network element (NEb).

4. The method according to any of the claims 1 to 3, wherein said freshness token (FRESH) comprises a random challenge (RAND) and said method comprises the steps of:
- said first cryptographic means (120) generating an expected response (XRES) based on said shared secret key (K_{AB}) and said random challenge (RAND);
- providing said expected response (XRES) to said first network element (NEa);
- said second cryptographic means (220) generating a response (RES) based on said shared secret key (K_{AB}) and said provided random challenge (RAND);
- providing said response (RES) to said first network element (NEa);
- said first network element (NEa) authenticating said second network element (NEb) based on a comparison between said expected response (XRES) and said response (RES).

5. The method according to claim 4, wherein said first cryptographic means (120) comprises an Authentication and Key Agreement (AKA) algorithm (30) for generating said random challenge (RAND), said expected response (XRES) and said session key (K), and said second cryptographic means (220) comprises an AKA algorithm (30) for generating said response (RES) and said copy of said session key (K).

6. The method according to any of the claims 1 to 5, further comprising the steps of:

- said first network element (NEa) providing an identifier (ID_b) associated with said second network domain (200) to said first cryptographic means (120); and
- said second network element (NEb) providing an identifier (ID_a) associated with said first network domain (100) to said second cryptographic means (220).

7. The method according to claim 6, wherein said session key (K) and said copy of said session key (K) are generated based on at least one of said identifier (ID_a) associated with said first network domain (100) and said identifier (ID_b) associated with said second network domain (200).

8. The method according to claim 6 or 7, further comprising the steps of:

- said first cryptographic means (120) identifying said shared secret key (K_{AB}) based on said identifier (ID_b) associated with said second network domain (200); and
- said second cryptographic means (220) identifying said shared secret key (K_{AB}) based on said identifier (ID_a) associated with said first network domain (100).

9. The method according to any of the claims 1 to 8, wherein said first cryptographic means (120) is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said first network

domain (100) and said second cryptographic means (220) is an AAA server provided in a network node of said second network domain (200).

10. The method according to any of the claims 1 to 9, wherein said first network domain (100) shares a second secret key (K_{AC}) with a third network domain (300) comprising third cryptographic means (320) and at least a third network element (NE_{C1}, NE_{C2}, NE_{C3}).

11. The method according to any of the claims 1 to 10, wherein said first network domain (100) is managed by a first communications network operator and said second network domain (200) is managed by a second different communications network operator.

12. The method according to any of the claims 1 to 11, further comprising the step of intermittently replacing said shared secret (K_{AB}) by a new shared secret by basing a key agreement between said first network domain (100) and said second network domain (200) on said shared secret (K_{AB}).

13. A system of establishing a session key (K) shared between a first network element (NEa) of a first network domain (100) and a second network element (NEb) of a second network domain (200), said first network domain (100) sharing a secret key (K_{AB}) with said second network domain (200), said first network domain (100) comprises:

- first cryptographic means (120) for generating a freshness token (FRESH) and for generating a session key (K) based on said shared secret key (K_{AB}) and said generated freshness token (FRESH);
- means (22) for providing said session key (K) from said first cryptographic means (120) to said first network element (NEa); and
- means (22) for providing said freshness token (FRESH) to said second network domain (200), said second network domain (200) comprises:
- second cryptographic means (220) for generating a copy of said session key (K) based on said shared secret key (K_{AB}) and said provided freshness token (FRESH); and

- means (22) for providing said copy of said session key (K) from said second cryptographic means (220) to said second network element (NEb).

14. A system of enabling secure communication between a first network element (NEa) of a first network domain (100) and a second network element (NEb) of a second network domain (200), said first network domain (100) sharing a secret key (K_{AB}) with said second network domain (200), said first network domain (100) comprises:

- first cryptographic means (120) for generating a freshness token (FRESH) and for generating a session key (K) based on said shared secret key (K_{AB}) and said generated freshness token (FRESH);
- means (22) for providing said session key (K) from said first cryptographic means (120) to said first network element (NEa); and
- means (22) for providing said freshness token (FRESH) to said second network domain (200), said second network domain (200) comprises:
- second cryptographic means (220) for generating a copy of said session key (K) based on said shared secret key (K_{AB}) and said provided freshness token (FRESH); and
- means (22) for providing said copy of said session key (K) from said second cryptographic means (220) to said second network element (NEb), said first network element (NEa) comprises means (12) for conducting secure communication with said second network element (NEb) based said session key (K) and said second network element (NEb) comprises means (12) for conducting secure communication with said first network element (NEa) based on said copy of said session key (K).

15. The system according to claim 13 or 14, wherein said session key providing means (22) is adapted for securely providing said session key (K) from said first cryptographic means (120) to said first network element (NEa) and said session key copy providing means (22) is adapted for securely providing said copy of said session key (K) from said second cryptographic means (220) to said second network element (NEb).

16. The system according to any of the claims 13 to 15, wherein said freshness token (FRESH) comprises a random challenge (RAND) and said first cryptographic means (120) comprises means (34) for generating an expected response (XRES) based on said shared secret key (K_{AB}) and said random challenge (RAND) and said second cryptographic means (220) comprises means (34) for generating a response (RES) based on said shared secret key (K_{AB}) and said random challenge (RAND), said first network domain (100) comprises means (22) for providing said expected response (XRES) to said first network element (NEa) and said second network domain (200) comprises means (22) for providing said response (RES) to said first network element (NEa), wherein said first network element (NEa) comprises means (16) for authenticating said second network element (NEb) based on a comparison between said expected response (XRES) and said response (RES).

17. The system according to claim 16, wherein said first cryptographic means (120) comprises an Authentication and Key Agreement (AKA) algorithm (30) for generating said random challenge (RAND), said expected response (XRES) and said session key (K), and said second cryptographic means (220) comprises an AKA algorithm (30) for generating said response (RES) and said copy of said session key (K).

18. The system according to any of the claims 13 to 17, wherein said first cryptographic means (120) is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said first network domain (100) and said second cryptographic means (220) is an AAA server provided in a network node of said second network domain (200).

19. The system according to any of the claims 13 to 18, further comprising a third network domain (300) with third cryptographic means (320) and at least a third network element (NE_{C1}, NE_{C2}, NE_{C3}), said first network domain (100) and said third network domain (300) share a second secret key (K_{AC}).

20. The system according to any of the claims 13 to 19, wherein said first network domain (100) is managed by a first communications network operator and said second network domain (200) is managed by a second different communications network operator.

21. The system according to any of the claims 13 to 20, further comprising means (36) for intermittently replacing said shared secret (K_{AB}) by a new shared secret, said shared secret replacing means (36) is adapted for replacing said shared secret (K_{AB}) based on a key agreement between said first network domain (100) and said second network domain (200) using said shared secret (K_{AB}).

22. A network domain (100) comprising:

- a first network element (NEa), adapted for communication with a second network element (NEb) of an external network domain (200), said network domain (100) and said external network domain (200) sharing a secret key (K_{AB});
- cryptographic means (20) for generating a freshness token (FRESH) and for generating a session key (K) based on said shared secret key (K_{AB}) and said generated freshness token (FRESH);
- means (22) for providing said session key (K) from said cryptographic means (20) to said first network element (NEa); and
- means (22) for providing said freshness token (FRESH) to said external network domain (200), wherein said external network domain (200) comprises means (20) for generating a copy of said session key (K) for said second network element (NEb) based on said shared secret key (K_{AB}) and said provided freshness token (FRESH).

23. The network domain according to claim 22, wherein said session key providing means (22) is adapted for securely providing said session key (K) from said cryptographic means (20) to said first network element (NEa).

24. The network domain according to claim 22 or 23, wherein said freshness token (FRESH) comprises a random challenge (RAND) and said cryptographic means (20) comprises means (34) for generating an expected response (XRES) based on said shared secret key (K_{AB}) and said random challenge (RAND) and said external network domain (200) comprises means (34) for generating a response (RES) based on said shared secret key (K_{AB}) and said random challenge (RAND), said network domain (100) comprises means (22) for providing said expected response (XRES) to said first network element (NEa) and said external network domain (200) comprises means (22) for providing said response (RES) to said first network element (NEa), wherein said first network element (NEa) comprises means (16) for authenticating said second network element (NEb) based on a comparison between said expected response (XRES) and said response (RES).

25. The network domain according to any of the claims 22 to 24, wherein said cryptographic means (20) is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said network domain (100).

26. A network domain (200) comprising:

- a first network element (NEb), adapted for communication with a second network element (NEa) of an external network domain (100), said network domain (200) and said external network domain (100) sharing a secret key (K_{AB});
- cryptographic means (20) for generating a session key (K) based on said shared secret key (K_{AB}) and a freshness token (FRESH) provided from said external network domain (100); and
- means (22) for providing said session key (K) from said cryptographic means (20) to said first network element (NEb), wherein said external network domain (100) comprises means (20) for generating said freshness token (FRESH) and for generating a copy of said session key (K) for said second network element (NEa) based on said shared secret key (K_{AB}) and said generated freshness token (FRESH).

27. The network domain according to claim 26, wherein said session key providing means (22) is adapted for securely providing said session key (K) from said cryptographic means (20) to said first network element (NEb).

28. The network domain according to claim 26 or 27, wherein said freshness token (FRESH) comprises a random challenge (RAND) and said cryptographic means (20) comprises means (34) for generating a response (RES) based on said shared secret key (K_{AB}) and said random challenge (RAND) and said external network domain (100) comprises means (34) for generating an expected response (XRES) based on said shared secret key (K_{AB}) and said random challenge (RAND) and means (22) for providing said expected response (XRES) to said second network element (NEa), said network domain (200) comprises means (22) for providing said response (RES) to said second network element (NEa), wherein said response (RES) and said expected response (XRES) enables said second network element (NEa) to authenticate said first network element (NEb).

29. The network domain according to any of the claims 26 to 28, wherein said cryptographic means (20) is an Authentication, Authorization and Accounting (AAA) server provided in a network node of said network domain (200).
